National Infrastructure Protection Center CyberNotes

Issue #2002-01 *January 14, 2002*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC web site at **http://www.nipc.gov**.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, D.C., 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between December 7, 2001 and January 11, 2002. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Abe Timmerman[1]	Unix	zml.cgi	A Directory Traversal vulnerability exists, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	zml.cgi File Disclosure	Medium	Bug discussed in newsgroups and web sites. Vulnerability can be exploited via a web browser.
Activestate[2]	Windows 95/98/ME /NT 4.0/2000, Unix	ActivePerl 5.6.1	A vulnerability exists when a request is sent to the server for a non-existent '.pl file,' which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	ActivePerl Path Revealing	Medium	Bug discussed in newsgroups and web sites. There is no exploit code required.
Adcycle. com[3]	Unix	Adcycle 1.12-1.17	A vulnerability exists in the AdCycle scripts, which could let a remote malicious user manipulate the MySQL database.	No workaround or patch available at time of publishing.	AdCycle Remote SQL Query Modification	Medium	Bug discussed in newsgroups and web sites. There is no exploit code required.
AFTPD[4]	Unix	AFTPD 5.4.4	A vulnerability exists due to the way input is handled, which could let an unauthorized remote malicious user obtain sensitive information and elevated privileges.	No workaround or patch available at time of publishing.	AFTPD Home Directory Change Core Dump	Medium	Bug discussed in newsgroups and web sites. There is no exploit code required.
Agora.cgi[5]	Unix	Agora.cgi 3.3e	A Cross-Site Scripting vulnerability exists because the 'Agora.cgi' script does not properly filter HTML tags, which could let an unauthorized malicious user insert malicious content into existing web pages.	No workaround or patch available at time of publishing.	Agora.CGI Cross-Site Scripting	**High**	Bug discussed in newsgroups and web sites. Exploit has been published.

[1] Blackshell Security Advisory No2, December 31, 2001.

[2] Securiteam, January 5, 2002.

[3] Bugtraq, December 25, 2001.

[4] Bugtraq, January 7, 2002.

[5] Securiteam, December 22, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Aktivate[6]	Unix	Aktivate 1.03	A Cross-Site Scripting vulnerability exists, which could let an unauthorized remote malicious user write malicious scripts, steal cookies, and modify the content of the site.	No workaround or patch available at time of publishing.	Aktivate Shopping Cart Cross-Site Scripting	**High**	Bug discussed in newsgroups and web sites. Exploit has been published.
Allaire[7]	Windows NT 4.0	Forums 2.0.4, 2.0.5, 3.0, 3.1	A vulnerability exists in the way new messages are posted, which could let an authorized malicious user impersonate a valid user.	No workaround or patch available at time of publishing.	Forums! Insecure User Validation Message Posting	Medium	Bug discussed in newsgroups and web sites. There is no exploit code required.
America OnLine, Incorporated[8]	Windows 95/98/ME /CE/NT 4.0/2000	AOL Instant Messenger 4.0-4.7	A Denial of Service vulnerability exists in AIM if an instant message containing an unusual number of character fonts is sent. This vulnerability may also affect Netscape's AIM client.	No workaround or patch available at time of publishing.	AOL Instant Messenger Font Denial of Service	Low	Bug discussed in newsgroups and web sites. There is no exploit code required.
America OnLine, Incorporated[9]	Windows 2000	AOLserver 3.4.2 Win32	A vulnerability exists because access control requests are not handled properly, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	AOLServer Password Protected File Arbitrary Read Access	Medium	Bug discussed in newsgroups and web sites. There is no exploit code required.

[6] Bugtraq, December 18, 2001.
[7] Bugtraq, January 8, 2002.
[8] Bugtraq, December 31, 2001.
[9] NTBugtraq, January 6, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
America OnLine, Incorporated[10]	Windows 95/98/ME/NT 4.0/2000, XP	AOL Instant Messenger 4.3-4.8.2616	A buffer overflow vulnerability exists due to the way AIM parses a game request, which could let a remote malicious user penetrate a victim's system without any indication as to who performed the attack.	"AOL has made changes to our instant messaging infrastructure to resolve the issue. Because these changes were made to the AOL infrastructure, all users automatically take advantage of the fix without the need of obtaining a patch or new client software."	AOL Instant Messenger Remote Buffer	**High**	Bug discussed in newsgroups and websites. Exploit script has been published. Vulnerability has appeared in the press and other public media.
Apache Group[11]	Unix	Apache 1.3.11, 1.3.12, 1.3.14, 1.3.17-1.3.20, 1.3.22	A Denial of Service vulnerability exists if an entry for a previously existing log directory is still present in the configuration file.	No workaround or patch available at time of publishing.	Apache Non-Existent Log Directory Denial Of Service	Low	Bug discussed in newsgroups and web sites. There is no exploit code required.
Apache Group[12]	Windows 95/98/NT 4.0/2000	Apache 1.3.11win32-1.3.20win32	A vulnerability exists in the default configuration of the Apache PHP.EXE binary, which could let an unauthorized remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Apache Win32 PHP.EXE Remote File Disclosure	**High**	Bug discussed in newsgroups and web sites. Exploits have been published.
Apple[13]	MacOS X 10.0, 10.1, 10.1.1, 10.1.2	MacOS X 10.0-10.1.2	A vulnerability exists when a user establishes a PPP connection and a 'ps' command is executed, which could let a malicious user obtain authentication information.	No workaround or patch available at time of publishing.	Mac OS X PPP Authentication Credentials Disclosure	Medium	Bug discussed in newsgroups and web sites. There is no exploit code required.

[10] w00w00 Security Development, January 2, 2002.

[11] Bugtraq, January 6, 2002.

[12] Securiteam, January 4, 2002.

[13] SecurityFocus, December 29, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Atmel[14]	Multiple	Atmel Firmware 1.3	A Denial of Service vulnerability exists f a SNMP read request is sent with a community string other than 'public', or an unknown OID key.	The vendor suggested the following: For customers that have earlier versions, new code is available at: ftp://ftp.linksys.com/pub/network/wap11fw14g5.exe The new utility is also required to use this firmware, also available at: ftp://ftp.linksys.com/pub/network/wap11sw.exe.	Atmel SNMP public Community or Unknown OID Denial of Service	Low	Bug discussed in newsgroups and web sites.
BEA Systems[15]	Windows NT 4.0/2000, Unix	Weblogic Server 6.1, 6.1SP1	A Denial of Service vulnerability exists when numerous URL requests for a MS-DOS device appended with a .jsp extension are submitted.	Upgrade to Service Pack 2 available at: http://commerce.beasys.com	WebLogic Server DOS Device Denial of Service	Low	Bug discussed in newsgroups and web sites. There is no exploit code required.
Boozt![16]	Unix	Boozt! Standard 0.9.8	A buffer overflow vulnerability exists when a new banner is crated with arbitrary characters of excessive length, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Boozt! Buffer Overflow	**High**	Bug discussed in newsgroups and web sites.
BrowseFTP[17]	Windows 95/NT 4.0	BrowseFTP Client 1.62	A buffer overflow vulnerability exists if the FTP server '220' response is of excessive length, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	BrowseFTP Client Buffer Overflow	**High**	Bug discussed in newsgroups and web sites. Exploit script has been published.

[14] VIGILANTe Advisory 2001003, December 21, 2001.

[15] KPMG-2002003, January 8, 2002.

[16] Securiteam, January 8, 2002.

[17] SecurityFocus, January 4, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
BSCW[18]	Windows NT 4.0/2000, Unix	BSCW 3.4, 4.0	Multiple vulnerabilities exist: a vulnerability exists because some shell metacharacters are not filtered, which could let a malicious user execute arbitrary commands; and a vulnerability exists because the default installation allows users to self-register, potentially allowing untrusted users to access the service.	Upgrade available at: **http://bscw.gmd.de/Download.html** There is no workaround or patch for the Insecure Default Installation vulnerability.	BSCW Remote Command Execution and Insecure Default Installation	**High**	Bug discussed in newsgroups and web sites. There is no exploit code required for the Remote Command Execution Vulnerability. Exploit has been published for the Insecure Default Installation vulnerability.
CacheFlow[19]	Multiple	CacheOS, 3.1.02-3.1.20	A vulnerability in the web admin interface exists when a certain request is sent, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	CacheOS Web Administration Arbitrary Cached Page Code Leakage	Medium	Bug discussed in newsgroups and web sites. Exploit has been published.
Caldera Systems[20]	Unix	UnixWare 7.1.0	A vulnerability exists in the CDE DTLogin, which could let a malicious user overwrite files and gain elevated privileges.	No workaround or patch available at time of publishing.	UnixWare CDE DTLogin Log Directory Insecure Permissions	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[18] Bugtraq, January 3, 2002.
[19] Svindel.net Security Advisory, January 8, 2002.
[20] Bugtraq, January 8, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Cherokee[21]	Unix	Cherokee HTTPD 0.2.0-0.2.6, 0.15- 0.1.6, 0.1.0	Multiple vulnerabilities exist: a Directory Traversal vulnerability exists which could let a remote malicious user obtain sensitive information; the Cherokee web server fails to drop root privileges after it binds to port 80, which could let a remote malicious user compromise root; and a vulnerability exists because shell metacharacters are not filtered from web requests, which could let a remote malicious user execute arbitrary code.	Upgrade available at: **http://aurora.esi.uem.es/~alo/cherokee/Cherokee-0.2.7.tar.gz**	Cherokee HTTPD Multiple Vulnerabilities	Medium/ **High** **(High for the root privileges and unfiltered meta-character vulnerabilities.)**	Bug discussed in newsgroups and websites. Directory Traversal vulnerability and Remote Command Execution Vulnerability can be exploited via a web browser. There is no exploit code required for the Insecure Privilege Release vulnerability.
Cisco Systems[22]	Multiple	Cisco ubr920, ubr924, ubr925	A vulnerability exists in the MIB default community strings, which could let a remote malicious user obtain sensitive information or change the router configuration.	No workaround or patch available at time of publishing.	Cisco Cable Access Router MIB Community Default Passwords	Medium	Bug discussed in newsgroups and web sites. There is no exploit code required.

[21] GOBBLES Security Advisory, December 29, 2001.

[22] HHC Network, January 3, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Cisco Systems[23]	Windows 95/98/ME /NT 4.0/2000	Cisco SN 5420 Storage Router 1.1(2)-(5)	Multiple vulnerabilities exist: a vulnerability which lets you read the stored configuration file from the Storage Router without any authorization, which could let a malicious user obtain access to the configuration file; a Denial of Service vulnerability exists when a HTTP request with large headers is sent; and a Denial of Service vulnerability exists when a fragmented packet is sent over the gigabit interface.	Upgrade available at: **http://www.cisco.com**.	Cisco SN 5420 Storage Router Multiple Vulnerabilities	Low/ Medium	Bug discussed in newsgroups and web sites. There is no exploit code required.
Citrix[24]	Windows, MacOS, Unix	ICA Client for Windows 6.1	A vulnerability exists when an ICA file is referenced within a web page, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Citrix ICA Client Automatic Remote Code Execution	**High**	Bug discussed in newsgroups and web sites. There is no exploit code required.
Datawizard Technologies[25]	Windows 95/98/NT 4.0/2000	FtpXQ 2.0, 2.1	A vulnerability exists in the default accounts included with FtpXQ, which could let a remote malicious user obtain sensitive information.	The vendor has acknowledged this issue and will change the default access to be read only.	FtpXQ Privileged Default Account Permissions	Medium	Bug discussed in newsgroups and web sites. There is no exploit code required.
DayDream[26]	Unix	DayDream BBS 2.9-2.13	Several buffer overflow vulnerabilities exist in some of the control codes when they contain extremely large parameters, which may let a remote malicious user execute arbitrary code.	Upgrade available at: **http://daydream.iwn.fi/download.html**	DayDream BBS Control Code Multiple Buffer Overflow	**High**	Bug discussed in newsgroups and web sites.

[23] Cisco Security Advisory, January 9, 2002.

[24] Kikkert Security Advisory, December 13, 2001.

[25] Securiteam, December 19, 2001.

[26] Securiteam, January 3, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
DeleGate[27]	Windows 95/98/ME /NT 4.0/2000, Unix	DeleGate 7.7.0, 7.7.1	A Cross-Site Scripting vulnerability exists because HTML tags are not filtered from links to error pages, which could let a malicious user insert malicious JavaScript code.	Upgrade available at: **http://www.delegate.org/delegate/**	DeleGate Cross-Site Scripting	**High**	Bug discussed in newsgroups and web sites. Exploit has been published.
D-Link[28]	Multiple	DWL-1000AP Firmware 3.2.28 #483	Two vulnerabilities exist: a vulnerability exists because the administrative password is stored in plaintext, which could let al malicious user gain access to the wireless network, change the configuration of the device, or cause a Denial of Service; and a vulnerability exists because the default read-only SNMP community string entitled "public" is hard-coded and cannot be changed with the configuration interface, which could let a malicious user obtain sensitive information	No workaround or patch available at time of publishing.	DWL-1000AP Wireless LAN Access Point Plaintext Password and Public Community	Medium	Bug discussed in newsgroups and web sites. Vulnerability can be exploited with a SNMP client.
ELSA[29]	Multiple	Lancom 1100 Office	A vulnerability exists because the web interface does not require authentication, which could let a remote malicious user obtain RAS passwords, change routing tables and place a modified firmware to sniff data.	No workaround or patch available at time of publishing.	Lancom 1100 Office Insecure Web Administration	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.

[27] SNS Advisory No.47, December 28, 2001.

[28] Bugtraq, December 21, 2001.

[29] Phoenix Sistemi Security Advisory, December 26, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
FAQ Manager[30]	Unix	FAQ Manager.cgi 2.0-2.2.5	A vulnerability exists because certain types of input from incoming web requests are not properly filtered, which could let a malicious user obtain sensitive information.	Upgrade available at: **http://www.fourteenminutes.com/code/faqmanager/FAQmanager_2.2.6.zip**	FAQManager.CGI NULL Character Arbitrary File Disclosure	Medium	Bug discussed in newsgroups and web sites. Vulnerability can be exploited via a web browser.
FAQ Manager[31]	Windows, Unix	FAQ Manager.cgi 2.0-2.2.6	A Directory Traversal vulnerability exists because input is not properly filtered, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	FAQManager.CGI Directory Traversal	Medium	Bug discussed in newsgroups and web sites. Vulnerability can be exploited via a web browser.
FreeBSD[32]	Unix	FreeBSD 4.2-4.4	A vulnerability exists when the 'pkg_add' package is executed, which could let a malicious user remove the data in directories, or obtain elevated privileges.	Patch available at: **ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-02:01/pkg_add.patch**	FreeBSD Package Add Insecure Temporary Directory Creation	Medium	Bug discussed in newsgroups and web sites.

[30] Securiteam, January 9, 2002.
[31] Bugtraq, January 7, 2002.
[32] FreeBSD Security Advisory, FreeBSD-SA-02:01, January 7, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Geeklog[33]	Windows NT 4.0/2000, Unix	Geeklog 1.3	A vulnerability exists in the GroupAdmin/UserAdmin Groups, which could let a malicious user obtain unprivileged access to gain admin rights.	**Workaround:** "If you have already installed a fresh version of Geeklog 1.3 then you need to edit the user with a uid of 13. To get that, do a "SELECT username FROM users WHERE uid = 13" in your favorite MySQL editor. Then in the admin/users.php page edit that user and uncheck both the GroupAdmin Group AND the UserAdmin Group and be sure to leave the Normal User and Logged-in User boxes checked."	Geeklog New User Default Admin Privileges	**High**	Bug discussed in newsgroups and web sites. There is no exploit code required.
GPM[34]	Unix	GPM 1.17.8	A format string vulnerability exists, which could let a malicious user execute arbitrary code with root privileges.	Upgrade available at: **http://security.debian.org/dists/stable/updates/main/**	GPM-Root Format String	**High**	Bug discussed in newsgroups and web sites.
Hardcore Software[35]	Unix	Anti-Web HTTPD 2.2	A Denial of Service vulnerability exists when a specially crafted script is submitted to the daemon.	Upgrade available at: **http://hardcoresoftware.cjb.net/awhttpd/awhttpd-2.2.1.tgz**	Anti-Web HTTPD Script Engine File Opening Denial Of Service	Low	Bug discussed in newsgroups and web sites. Exploit has been published.
Hardcore Software[36]	Unix	Anti-Web HTTPD 2.2	A heap overflow vulnerability exists when a specially crafted script is parsed by the scripting engine, which could let a malicious user execute arbitrary code.	Upgrade available at: **http://hardcoresoftware.cjb.net/awhttpd/awhttpd-2.2.1.tgz**	Anti-Web HTTPD Script Engine Heap Overflow	**High**	Bug discussed in newsgroups and web sites.

[33] Bugtraq, January 3, 2002.

[34] Debian Security Advisory, DSA-095-1, December 27, 2001.

[35] AngryPacket Security Advisory, January 3, 2002.

[36] Securiteam List Digest, January 8, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hewlett Packard Systems[37]	Unix	HP-UX 10.20 Series 800, Series 700, 11.0, 11.11, HP-UX (VVOS) 11.04	A Denial of Service vulnerability exists when a malicious user maps a file to a memory buffer using the mmap() system call.	Patch available at: **http://itrc.hp.com**	HP-UX mmap() Denial of Service	Low	Bug discussed in newsgroups and web sites.
Hosting Controller[38]	Windows NT 4.0/2000	Hosting Controller 1.4.1	Multiple Directory Traversal vulnerabilities exist, which could let a malicious user obtain sensitive information and gain administrative privileges.	No workaround or patch available at time of publishing.	Hosting Controller Multiple Vulnerabilities	**High**	Bug discussed in newsgroups and web sites. There is no exploit code required.
Hughes Technology[39]		Mini SQL 2.0.10-2.0.13	A Denial of Service vulnerability exists when a select statement is issued with large character arrays against the database tables.	No workaround or patch available at time of publishing.	Hughes Technologies Mini SQL Denial of Service	Low	Bug discussed in newsgroups and web sites. There is no exploit code required.
Infopop[40]	Unix	Ultimate Bulletin Board 5.4.7e, 5.43, 6.0Beta-6.0.3, 6.0.4f, 6.2.0 Beta Release 1.0	A Cross-Site Scripting vulnerability exists due to insufficient input validation, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	Ultimate Bulletin Board Cross-Site Scripting	**High**	Bug discussed in newsgroups and web sites. Exploit has been published.

[37] Hewlett-Packard Company Security Bulletin, HPSBUX0201-178, January 7, 2002.

[38] Securiteam, January 8, 2002.

[39] SecurityFocus, December 27, 2001.

[40] Bugtraq, January 9, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
IpSwitch[41]	Windows NT 4.0/2000	IMail 6.1-6.4, 7.0.1-7.0.4	A vulnerability exists with the authentication process for the administration tool, which could let a malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	IMail Domain Administration Privilege Escalation	**High**	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
John Hardin[42]	Multiple	Procmail Email Sanitizer 1.131, 1.132	A vulnerability exists in the way certain recursive multipart MIME attachments are decoded, which could let a malicious user evade the e-mail filter.	Update available at: **http://www.impsec.org/email-tools/html-trap.procmail.gz**	Procmail Email Sanitizer Multipart Mime Recognition	Medium	Bug discussed in newsgroups and web sites.
KDE Project[43]	Unix	KDEUtils 2.2-2, 2.2	A vulnerability exists in the klprfax_filter program, which could let a malicious user overwrite and create files with root privileges.	No workaround or patch available at time of publishing.	KDE2 KDEUtils KLPRFax_Filter Insecure Temporary File Creation	**High**	Bug discussed in newsgroups and web sites. There is no exploit code required.
Lebios[44]	Multiple	phptonuke.php 1.0	A vulnerability exists in the phptonuke.php script, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	PHPNuke AddOn PHPToNuke.PHP Cross-Site Scripting	**High**	Bug discussed in newsgroups and web sites. Exploit has been published.
Les VanBrunt[45]	Unix	AdRotate Pro 2.0	A vulnerability exists in SQL statements when certain characters are included in the user input, which could let a malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	AdRotate Pro SQL Injection	**High**	Bug discussed in newsgroups and web sites. Vulnerability can be exploited via a web browser.

[41] Securiteam, January 2, 2002.

[42] SecurityFocus, January 8, 2002.

[43] Securiteam, December 28, 2001.

[44] Bugtraq, January 6, 2002.

[45] ———Bugtraq, December 23, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
LIDS[46]	Unix	LIDS 1.1 & prior	A vulnerability exists in the "Linux Intrusion Detection System" security patch for the Linux kernel, which could let a malicious user gain unrestricted root privileges.	Patch available at: **http://www.lids.org/download/LIDS-security-patch-0.10.1-2.2.20.diff.gz**	LIDS Capability Leakage via LD_ PRELOAD	**High**	Bug discussed in newsgroups and web sites.
Linksys Group[47]	Unix	EtherFast BEFN2PS4 Router , BEFSR81 Router	Two vulnerabilities exist: a vulnerability exists due to a design issue that will route SNMP Trap information to any address, which could let a remote malicious user obtain sensitive information or create a Denial of Service; and a vulnerability exists due to a default community string of "public," which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Linksys DSL Router SNMP Trap System Arbitrary Sending and Default SNMP Community String Vulnerabilities	Low/ Medium	Bug discussed in newsgroups and web sites. Vulnerability may be exploited with one of the many available SNMP query tools.
Mandrake Soft[48]	Unix	Linux Mandrake 8.0, 8.0 ppc, 8.1 ia64, 8.1	A vulnerability exists due to insecure permissions on configuration files, which could let a malicious user obtain sensitive information.	Upgrade available at: **ftp://fr2.rpmfind.net/linux/Mandrake/updates/**	Mandrake Bind 9 Package Insecure File Permissions	Medium	Bug discussed in newsgroups and web sites.
Marcus S. Xenakis[49]	Unix	Unix Manual 1.0	A vulnerability exists in the script manual.php when metacharacters are included in the script's input, which could let a malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	manual.php Arbitrary Shell Command Execution	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Markus Kliegl[50]	Unix	mod_bf 0.2	A buffer overflow vulnerability exists in the 'mod_bf' interpreter, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	mod_bf Buffer Overflow	**High**	Bug discussed in newsgroups and web sites.

[46] TESO Security Advisory, January 9, 2002.

[47] Bugtraq, January 6, 2002.

[48] Mandrake Linux Security Update Advisory, MDKSA-2002:001, January 9, 2002.

[49] Bugtraq, December 15, 2001.

[50] Securiteam, December 25, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Michael Lamont[51]	Windows 95/98/NT 4.0/2000	Savant WebServer 3.0	A Denial of Service vulnerability exists if a request is submitted that contains an unusual number of arbitrary characters.	No workaround or patch available at time of publishing.	Savant Web Server Long Request Denial of Service	Low	Bug discussed in newsgroups and web sites. There is no exploit code required.
Microsoft[52]	Unix	Internet Explorer 5.0 SP1 Solaris	A remote Denial of Service vulnerability exists if a Chinese language web page is displayed and rapidly scrolled. This may also happen if the IE Window is maximized.	No workaround or patch available at time of publishing.	Internet Explorer for Solaris X Server Denial of Service	Low	Bug discussed in newsgroups and web sites.
Microsoft[53]	Windows 95/98/ME /NT 4.0/2000	Excel 97, 97SR2&2, 2000, 2002	A vulnerability exists in one of Excel's security implementations, which could let a malicious user bypass password protected data and obtain sensitive information.	No workaround or patch available at time of publishing.	Excel Spreadsheet Data Password Protection Bypass	Medium	Bug discussed in newsgroups and web sites. There is no exploit code required. Vulnerability has appeared in the press and other public media.
Microsoft[54]	Windows 95/98/ME /NT 4.0/2000	Internet Explorer 5.0, 5.01, Internet Explorer 5.01SP1&2, 5.5, 5.5SP1&2	A vulnerability exists when script code includes a file outside of the document it is embedded in and the file does not exist, which could let a malicious user obtain sensitive information.	Upgrade to Internet Explorer 6.0.	Internet Explorer JavaScript Local File Enumeration	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[51] VulnWatch, January 5, 2002.

[52] Bugtraq, December 20, 2001.

[53] SecurityFocus, December 20, 2001.

[54] Bugtraq, January 3, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[55]	Windows 95/98/ME /NT 4.0/2000	Internet Explorer 5.5, 5.5SP1&2, 6.0	A vulnerability exists due to a violation of the 'same origin policy', which could let a malicious user steal cookies, read local files that are parse-able by Internet Explorer, and spoof sites.	No workaround or patch available at time of publishing.	Internet Explorer Same Origin Policy Violation	**High**	Bug discussed in newsgroups and web sites. Exploits have been published. Vulnerability has appeared in the press and other public media.
Microsoft[56]	Windows 95/98/ME /NT 4.0/2000	Internet Explorer 5.5, 5.5SP1&2, 6.0	A Denial of Service vulnerability exists when a malicious web site operator designs a web page containing JavaScript designed to cause a continuous refresh.	No workaround or patch available at time of publishing.	Internet Explorer Refresh Denial of Service	Low	Bug discussed in newsgroups and web sites.
Microsoft[57]	Windows 95/98/ME /NT 4.0/2000	Internet Explorer 5.5, 5.5SP1&2, 6.0	A vulnerability exists when the 'GetObject()' JavaScript function is used with the object 'htmlfile', which could let a remote malicious user read local files and possibly execute arbitrary code.	No workaround or patch available at time of publishing.	Internet Explorer GetObject File Disclosure	**High**	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the press and other public media.
Microsoft[58]	Windows 95/98/ME /NT 4.0/2000	Internet Explorer 5.5, 5.5SP1&2, 6.0	A Denial of Service vulnerability exists if the modeless dialog method is passed in an HTML document.	No workaround or patch available at time of publishing.	Internet Explorer Modeless Dialog Denial of Service	Low	Bug discussed in newsgroups and websites.

[55] Securiteam, December 20, 2001.

[56] SecurityFocus, December 21, 2001.

[57] Georgi Guninski Security Advisory #52, January 1, 2002.

[58] SecurityFocus, January 7, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[59]	Windows 98/98SE/ ME/XP	Windows 98, 98SE, ME, XP	Three vulnerabilities exist in the Universal Plug and Play (UPnP) feature: a buffer overflow vulnerability exists in one of the components that handles NOTIFY directives, which could let a remote malicious user execute arbitrary code with administrative privileges; and a remote Denial of Service and Distributed Denial of Service vulnerability exists in the Simple Service Discovery Protocol (SSDP) that is a component of UPnP because steps to obtain information on a newly discovered device are not sufficiently limited.	Frequently asked questions regarding these vulnerabilities and the patches can be found at: **http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-059.asp**	Windows UPnP NOTIFY Buffer Overflow and Denial of Service Distributed Denial of Service CVE Names: CAN-2001-0876, CAN-2001-0877	Low/**High** **(High for the buffer overflow UPnP vulnerability.)**	Bug discussed in newsgroups and websites. There is no exploit code required for the buffer overflow vulnerability. Vulnerability has appeared in the press and other public media.
Microsoft[60]	Windows 98/ME/NT 4.0/2000	Internet Explorer 6.0	A vulnerability exists in the 'Microsoft.XMLHTTP' component, which could let a remote malicious user obtain sensitive information.	Unofficial workaround (Bugtraq): Disable active scripting.	Internet Explorer XMLHTTP File Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[59] Microsoft Security Bulletin, MS01-059, December 20, 2001.

[60] Bugtraq, December 15, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[61]	Windows NT 4.0/2000, XP	SQL Server 7.0, 2000	Two vulnerabilities exist: a Denial of Service exists due to a format string vulnerability in the C Runtime Library; and buffer overflow vulnerabilities exist in several built-in text formatting and printing functions, which could let a malicious user either execute arbitrary code in the security context of the SQL Server service or cause the SQL Server service to fail.	Because the two vulnerabilities have different root causes, there are separate patches for each. Microsoft recommends that the SQL Server patch be applied to all affected servers. However, they recommend that customers carefully weigh whether they need to apply the C runtime patch. Frequently asked questions and patches can be found at: **http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-060.asp**	SQL Server C Runtime Library Format String and Buffer Overflow CVE Names: CAN-2001-0542, CAN-2001-0879	Low/ **High** **(High for the buffer overflow vulnera-bilities.)**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Microsoft[62]	Windows XP	Windows XP	A vulnerability exists when the system is locked, which could let a malicious user execute administrator owned applications by using hotkey combinations.	Temporary workaround (Securiteam): Disable hot keys.	Windows XP Unauthorized Hotkey Program	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[61] Microsoft Security Bulletin, MS01-060, December 20, 2001.

[62] Securiteam, December 22, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[63]	Windows XP	Windows XP	Three security vulnerabilities exist: a vulnerability exists if the fast switching feature is used multiple times to cycle to the same user account and the account lockout threshold is set, which could let a malicious user lockout all other users other than the administrator; a vulnerability exists in the "Password Reset Disk" feature, that in certain conditions the user may not be able to reset his password and the only solution is the reset password feature available to the Administrator; and a vulnerability exists in the Remote Desktop (RD) client because the recently used username that has been used to logon with the RD client is sent in plaintext, which could let a malicious user capture traffic on a network and discover user account names.	No workaround or patch available at time of publishing.	Windows XP Multiple Security Vulnerabilities	Medium	Bug discussed in newsgroups and websites.
Mirabilis[64]	Windows 95/98/ME/NT 4.0/2000	ICQ 2000.0b Build 3278, 2000.0A	A buffer overflow vulnerability exists in ICQ's handling of specially formatted communications, which could let a remote malicious user crash the system and possibly execute arbitrary code.	No workaround or patch available at time of publishing.	ICQ Remote Buffer Overflow	Low/**High** **(High if arbitrary code is executed)**	Bug discussed in newsgroups and websites.

[63] Securiteam, December 21, 2001.

[64] SecurityFocus, January 8, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Mozilla Project[65]	Windows 95/98/NT 3.5.1/4.0	BugZilla 2.4, 2.6, 2.8, 2.10, 2.12, 2.14	Multiple vulnerabilities exist: a vulnerability in the 'process_bug.cgi' script, which could let a malicious user add bug comments as any other user; a vulnerability in the 'post_bug.cgi' script, which could let a malicious user add bug comments as any other user; a vulnerability exists in the pulldown menus in the 'show_bug.cgi' script, which could let a malicious user obtain sensitive information; a vulnerability exists when a bad login to 'doeditvotes.cgi' occurs, which could let a malicious user obtain sensitive information; a vulnerability exists in the 'buglist.cgi' script due to lack of input validation, which could let a remote malicious user execute arbitrary commands; a vulnerability exists in the 'UserPrefs.cgi' groupsee form, which could let a malicious user manipulate forms with their own information; a vulnerability exists in the 'buglist.cgi' script, which may let a remote malicious user modify the logic of an SQL query; and a vulnerability exists in the 'longlist.cgi' script, which could let a malicious user pass untrusted input to the database.	Upgrade available at: **http://ftp.mozilla.org/pub/webtools/bugzilla-LATEST.tar.gz**	BugZilla Multiple Vulnerabilities	Medium/ **High** **(High for the buglist.cgi script vulnera-bility.)**	Bug discussed in newsgroups and websites. There is no exploit code required.

[65] SecurityFocus, January 8, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Mozilla Project[66]	Unix	Browser 0.8	A symbolic link vulnerability exists because the '.nmsc-0-lock' file is created in the /tmp directory without checking for an existing file or symbolic link, which could let a malicious user overwrite the linked file.	No workaround or patch available at time of publishing.	Mozilla Predictable Temporary File Symbolic Link Attack	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Mozilla Project[67]	Windows 95/98/NT 3.5.1/4.0	Bugzilla 2.4, 2.6, 2.8, 2.10, 2.12, 2.14	A vulnerability exists in the implementation of LDAP, which could let a malicious user gain unauthorized access. This is only an issue if Bugzilla is configured to use LDAP authentication.	Upgrade available at: **http://ftp.mozilla.org/pub/webtools/bugzilla-LATEST.tar.gz**	BugZilla LDAP Authentication Bypass	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

Multiple Vendors[68]	Multiple	Links Links 0.96;
		University of Kansas Lynx 2.7, 2.8, 2.8.4;
		W3M W3M 0.1.3, 0.1.4, 0.1.6-0.1.10,
		W3M 0.2-0.2.3
			A vulnerability exists because certain web browsers have implemented SSL functionality without including the ability to verify certificates, which could let a malicious user spoof a trusted site, or implement a man-in-the-middle attack.	No workaround or patch available at time of publishing.	Multiple Vendor SSL Certificate Validation	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

Multiple Vendors[69]	Unix	GNU GZip 1.3 -1.2.4a	A buffer overflow vulnerability exists because long file names are not properly handled, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	GZip Long File Name Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Multiple Vendors[70]	Unix	Linux kernel 2.2-2.2.20, 2.4-2.4.17	A security vulnerability exists in the encrypted loop device, which could let a malicious user modify the content of the encrypted device without being detected.	No workaround or patch available at time of publishing.	Linux Encrypted Loop Filesystem Replay Attack	Medium	Bug discussed in newsgroups and websites.

[66] SecurityFocus, December 28, 2001.

[67] SecurityFocus, January 8, 2002.

[68] SecurityFocus, January 7, 2002.

[69] Gobbles Security Advisory, December 18, 2001.

[70] Bugtraq, January 2, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[71], [72], [73], [74], [75], [76]	Unix	GNU glibc 2.0-2.2.4	A buffer overflow vulnerability exists in the 'glob()' function, which could let a malicious user execute arbitrary code.	**RedHat:** ftp://updates.redhat.com/ **Conectiva:** ftp://atualizacoes.conectiva.com.br/ **Engarde:** ftp://ftp.engardelinux.org/pub/engarde/stable/updates/ **Trustix:** ftp://ftp.trustix.net/pub/Trustix/updates/ **Mandrake Linux:** http://www.linux-mandrake.com/en/ftp.php3	Glibc File Globbing Heap Corruption CVE Name: CAN-2001-0886	**High**	Bug discussed in newsgroups and websites.
Mutt Development Team[77], [78], [79], [80], [81], [82], [83]	Unix	Mutt 0.93.2, 1.0.1, 1.2.5, 1.3.12, 1.3.16, 1.3.17, 1.3.22, 1.3.24	A buffer overflow vulnerability exists in the e-mail address handling routines, which could let a malicious user execute arbitrary code.	**Mutt:** ftp://ftp.mutt.org/pub/mutt/mutt-1.2.5.1.tar.gz **Debian:** http://security.debian.org/dists/stable/updates/main/ **Trustix:** http://www.trustix.net/pub/Trustix/updates/ **FreeBSD:** ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/ **Conectiva:** ftp://atualizacoes.conectiva.com.br/ **RedHat:** ftp://updates.redhat.com/ **SuSE:** ftp://ftp.suse.com/pub/suse/i386/update/	Mutt Address Handling Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[71] Red Hat Security Advisory, RHSA-2001:160-09, December 14, 2001.

[72] Conectiva Linux Security Announcement, CLA-2002:447, January 3, 2001.

[73] EnGarde Secure Linux Security Advisory, ESA-20011217-01, December 17, 2001.

[74] Trustix Secure Linux Security Advisory, TSLSA-2001-0029, December 19, 2001.

[75] Hewlett-Packard Company Security Bulletin, HPSBTL0112-008, December 17, 2001.

[76] Mandrake Linux Security Update Advisory, MDKSA-2001:095, December 19, 2001.

[77] Debian Security Advisory, DSA-096-1, January 2, 2002.

[78] Debian Security Advisory, DSA-096-2, January 3, 2002.

[79] Trustix Secure Linux Security Advisory #2002-0003, January 4, 2002.

[80] FreeBSD Security Advisory, FreeBSD-SA-02:04, January 6, 2002.

[81] Conectiva Linux Security Announcement, CLA-2002:449, January 7, 2002.

[82] Red Hat Security Advisory, RHSA-2002:003-10, January 7, 2002.

[83] SuSE Security Announcement, SuSE-SA:2002:001, January 7, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Namazu Project[84]	Unix	Namazu 2.0.7, 2.0.8	A Cross-Site vulnerability exists, which could let a malicious user inject arbitrary script code into pages generated by Namazu.	Upgrade available at: **ftp://updates.redhat.com/7.0/ja/os/**	Namazu Search System Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Netscape iPlanet[85]	Windows NT 4.0/2000, Unix	Enterprise Server 3.0-3.6, Edition 4.0, 4.1; iPlanet E-Commerce Solutions iPlanet Web Server 6.0, Enterprise Edition 4.0-4.1	A Denial of Service vulnerability exists when a malformed '?wp-html-rend' request is sent to a host with web publishing enabled.	**iPlanet:** **http://knowledgebase.iplanet.com/NASApp/ikb/cat?file=file/7761/DisRend.c**	Netscape Enterprise Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.

[84] Red Hat Security Advisory, RHSA-2001:162-04, December 7, 2001.

[85] CERT Vulnerability Note, VU#191763, January 8, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Netscape iPlanet[86]	Windows NT 4.0/2000, Unix	Enterprise Server 3.0-3.6, Edition 4.0, 4.1; iPlanet E-Commerce Solutions iPlanet Web Server 6.0, Enterprise Edition 4.0-4.1	A vulnerability exists when a request is submitted containing 'wp-force-auth,' which could let a malicious user obtain sensitive information.	The following solution has been taken from the Planet Knowledge Base Article ID: 7764: "When you enable web publishing, you should treat the web server as an environment that must be secured. Ensure that users follow proper password policies such as using hard to guess passwords. If intruder detection software is used, it should be configured to check for ?wp-force-auth requests. HTTP basic authentication is generally not considered a secure mechanism and should be run over a SSL-enabled port. In addition, access logs should be monitored for suspicious requests. A better alternative would be to use client certificates, which are much more secure."	Netscape Enterprise Web Server Brute Force Authentication Attacks	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Net-SNMP[87]	Unix	Net-SNMP 4.2.3	A heap overflow vulnerability exists in the 'snmpnetstat' client, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Net-SNMP snmpnetstat Remote Heap Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[86] CERT Vulnerability Note, VU#985347, January 8, 2002.

[87] Axioma Security Research Advisory, January 3, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Network Associates[88]	Windows 95/98/ME /NT 4.0/2000	PGP 7.0, 7.0.3, 7.0.4	A vulnerability exists in the PGP Outlook Plug-in that causes the Exchange Server to automatically save decrypted messages to the system disk without user notification when the recipient chooses to reply to a PGP encrypted message. This could create a false sense of security for users of this product.	Upgrade to 7.1.1.	PGP Outlook Plug-In Insecure Message Storage	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Nombas[89]	Windows, OS/2, Unix	ScriptEase: Webserver Edition 4.30d win3.x, 4.30d OS/2, 4.30d Netware 5, 4.30d ISAPI win32, 4.30d CGI/WINCGI win32, 4.30b solaris, ppc, Linux, Irix, HP-UX; FreeBSD	A vulnerability exists in the 'viewcode.jse' sample script, which could let a remote malicious user obtain sensitive information.	Novell Upgrade available at: **http://support.novell.com/servlet/tidfinder/2959615** Workaround: Delete the example script, viewcode.jse.	ScriptEase: Webserver Edition Default Script	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Novell[90]	Multiple	Groupwise 6.0, Groupwise Enhance-ment Pack 5.5	A vulnerability exists because GroupWise is installed with a default username and password that controls the servlet manager, which could let a remote malicious user obtain unauthorized access.	Unofficial workaround (Bugtraq): Change the password: Edit the SYS:\JAVA\SERVLETS\SERVLET.PROPERTIES file.	Groupwise Servlet Gateway Default Authentication	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[88] Securiteam, January 8, 2002.
[89] IRM Security Advisory 002, December 19, 2001.
[90] Bugtraq, December 15, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Oliver Rauch[91]	Unix	xSANE 0.81	A vulnerability exists because temporary files are created in the /tmp directory that have predictable file names, which could let al malicious user overwrite file contents.	Upgrade available at: **ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/i386/packages-5-current/graphics/xsane-0.82.tgz**	xSANE Insecure Temporary File Creation CVE Name: CAN-2001-0887	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Oracle Corporation[92]	Windows NT 4.0/2000, Unix	Oracle 9i Application Server	Two vulnerabilities exist: a buffer overflow vulnerability exists in the PL/SQL Apache module, which could let a remote malicious user execute arbitrary code (Windows NT/2000 systems code is executed with SYSTEM level privileges); and a Directory Traversal vulnerability exists on Windows NT/2000 operating systems in the PL/SQL Apache module. which could let a remote malicious user obtain sensitive information.	Patch available at: Oracle Patch 2128936 **http://metalink.oracle.com**	Oracle 9I Application Server PL/SQL Apache Module Buffer Overflow and Directory Traversal	Medium/ **High** **(High for the PL/SQL buffer overflow vulnerability.)**	Bug discussed in newsgroups and websites. Directory Traversal vulnerability can be exploited via a web browser.
Oracle Corporation[93]	Windows NT 4.0/2000, Unix	Oracle9iAS Web Cache 2.0.0.0-2.0.0.2, 2.0.0.2 NT	Multiple vulnerabilities exist: several remote Denial of Service vulnerabilities exist; a vulnerability exists due to unsafe permissions via '$ORACLE_HOME/webcache/bin/webcached,' which could let a malicious user obtain elevated privileges; and the password of the administrator account is stored in a world-readable file, which could let a malicious user obtain sensitive information.	Patch available at: Patch 2131605 **http://metalink.oracle.com**	Oracle9iAS Web Cache Multiple Vulnerabilities	Low/ Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[91] FreeBSD Security Advisory, FreeBSD-SA-01:68, December 17, 2001.

[92] NGSSoftware Insight Security Research Advisory, NISR20122001, December 21, 2001.

[93] Oracle Security Alert #27, December 28, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
PFinger[94]	Unix	PFinger 0.7.5-0.7.7	A format string vulnerability exists in both the server and the client, which could let a malicious user execute arbitrary code.	Upgrade available at: **http://www.xelia.ch/unix/pfinger/download**	PFinger Format String	**High**	Bug discussed in newsgroups and websites. Exploits have been published.
Plesk[95]	Unix	Plesk Server Administra-tor 1.0	A vulnerability exists due to an input validation error, which could let a remote malicious user obtain sensitive information.	Upgrade available at: **http://www.plesk.com/html/**	Plesk Server Administrator PHP Source Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Plumtree[96]	Multiple	Plumtree Corporate Portal 4.5	A Cross-Site scripting vulnerability exists in the script 'error.asp,' which could let a malicious user execute arbitrary JavaScript.	No workaround or patch available at time of publishing.	Plumtree Corporate Portal Cross Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Real Networks[97]	Windows 98/ME/NT 4.0/2000, XP	RealPlayer 8.0 Win32, 8.0 Unix	A buffer overflow vulnerability exists when a file is received with a malformed header, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	RealPlayer Media File Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
SQLData Systems[98]	Windows 95/NT 4.0	SQLData Enterprise Server 3.0	A buffer overflow vulnerability exists when a specially crafted request containing an unusually long string of characters is submitted, which could let a malicious user execute arbitrary code with system privileges.	No workaround or patch available at time of publishing.	SQLData Enterprise Server Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[94] INTEXXIA(c) Security Advisory, 1050-181201, December 18, 2001.

[95] TWLC Security Advisory, December 21, 2001.

[96] SecurityFocus, January 7, 2002.

[97] SecurityFocus, January 8, 2002.

[98] SecurityFocus, January 3, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Stunnel[99], [100]	Unix	Stunnel 3.15-3.21c	Format string vulnerabilities exist in each of the SMTP, POP, and NNTP client negotiations because unexpected user input is not properly handled, which could let malicious user execute arbitrary code.	**Engarde:** **http://ftp.engardelinux.org/pub/engarde/stable/updates/** **RedHat:** **ftp://updates.redhat.com/7.2/en/os/**	STunnel Client Negotiation Protocol Format String CVE Name: CAN-2002-0002	**High**	Bug discussed in newsgroups and websites.
Sun Micro Systems, Incoraporated[101]	Unix	Sun SMC 2.0	A vulnerability exists in the script that starts smcboot because adequate checking is not performed prior to creating a directory in /tmp, which could let a malicious user create a symoblic link to an arbitrary directory.	Patch available at: Sun Patch 109134-24, Sun Patch 109135-24 **http://sunsolve.sun.com**	Sun SMCBoot Insecure Temporary File Creation Directory Destruction	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Timecop[102]	Unix	WMCube/ GDK 0.98	A buffer overflow vulnerability exists when an object file greater than 64 bytes is loaded, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	WMCube/ GDK Object File Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
tinc[103]	Unix	tinc 1.0pre3, 1.0pre3	Multiple vulnerabilities exist due to no packet authentication, and the ability to insert random and chosen data, which could let a malicious user modify packets, replay them and learn plain text patterns.	No workaround or patch available at time of publishing.	tinc Multiple Vulnerabilities	Medium	Bug discussed in newsgroups and websites.

[99] EnGarde Secure Linux Security Advisory, ESA-20011227-01, December 27, 2001.

[100] Red Hat Security Advisory, RHSA-2002:002-10, January 3, 2002.

[101] Securiteam, December 28, 2001.

[102] Securiteam, December 21, 2001.

[103] Bugtraq, January 9, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Total PC Solutions[104]	Multiple	PHP Rocket Add-in for FrontPage 1.0	A Directory Traversal vulnerability exists, which may let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	PHP Rocket Add-in for FrontPage Directory Traversal	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
University of Cambridge[105], [106]	Unix	Exim 3.11-3.22, 3.30-3.33	A vulnerability exists when the local exim configuration directs or routes an address to a pipe transport without verifying that the local part is valid, which could let a remote malicious user rum arbitrary commands encoded in the local address.	**University of Cambridge:** http://www.exim.org **Debian:** http://security.debian.org/dists/stable/updates/main/ **RedHat:** ftp://updates.redhat.com/6.2/en/powertools/	Exim Pipe Hostname Arbitrary Command Execution	Medium	Bug discussed in newsgroups and websites.
University of Washington[107]	Unix	Pine 4.20, 4.21, 4.30, 4.33	A vulnerability exists in the way encapsulated environment variables in URLs are handled, which could let a malicious user execute arbitrary code.	**University of Washington:** ftp://ftp.cac.washington.edu/pine/pine.tar.Z **FreeBSD:** ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/i386/packages-4-stable/mail/pine-4.44.tgz	Pine Environment Variable URL Shell Interpreting	**High**	Bug discussed in newsgroups and websites.
VTun[108]	Unix	VTun 2.0-2.4, 2.5b1	A vulnerability exists due to the fundamental properties of ECB mode ciphers, which could let a malicious user modify packets, replay them, learn patterns of plain text, or easily guess low-entropy passwords.	No workaround or patch available at time of publishing.	VTun ECB Mode Encryption	Medium	Bug discussed in newsgroups and websites.

[104] Bugtraq, December 28, 2001.

[105] Debian Security Advisory, DSA 097-1, January 3, 2002.

[106] Red Hat Security Advisory, RHSA-2001:176-05, January 7, 2002.

[107] FreeBSD SecurityAdvisory, FreeBSD-SA-02:05, January 10, 2002.

[108] Securiteam, January 11, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Webmin[109]	Unix	Webmin 0.91	A Directory Traversal vulnerability exists, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Webmin Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
X-Chat[110]	Unix	X-Chat 1.4.2, 1.4.3	A vulnerability exists if a CTCP ping request is received that includes escaped newline characters and additional IRC commands, which could let a malicious user takeover channels.	Update available at: **http://www.xchat.org/ download.html**	X-Chat CTCP Ping Arbitrary Remote IRC Command Execution	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
YaBB[111]	Windows 95/98/NT 4.0/2000	YaBB 1 Gold Release, 1 Gold - SP 1, 9.1.2000, 9.11.2000	A Cross-Site Scripting vulnerability exists when HTML tags are inserted into image links in messages, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	YaBB Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
ZyXel[112]	Multiple	Prestige 681	A remote Denial of Service vulnerability exists when a Zyxel router receives fragmented packets through the DSL interface that are greater than 64 kilobytes.	No workaround or patch available at time of publishing.	ZyXel Prestige SDSL Router IP Fragment Reassembly	Low	Bug discussed in newsgroups and websites. Exploit has been published

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to

[109] ———Bugtraq, December 17, 2001.
[110] Securiteam, January 11, 2002.
[111] VulnWatch, January 9, 2002.
[112] Securiteam, December 19, 2001

continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a “High” threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between December 16, 2001 and January 11, 2002, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing**. During this period, 25 scripts, programs, and net-news messages containing holes or exploits were identified. *Note: At times, scripts/techniques may contain names or content that may be considered offensive.*

Date of Script (Reverse Chronological Order)	Script name	Script Description
January 11, 2002	Xchat.exploit	Exploit for the X-Chat CTCP Ping Arbitrary Remote IRC Command Execution vulnerability.
January 10, 2002	**Boozt.c**	**Script which exploits the Boozt! Buffer Overflow vulnerability.**
January 10, 2002	Buggyzilla.pl	Perl script which exploits two BugZilla vulnerabilities.
January 10, 2002	Irpas_0.10.tar.gz	A suite of routing protocol attack tools which sends custom routing protocol packets from the Unix command line.
January 9, 2002	2001-exploits.tg	A file from Packet Storm that contains new exploits for 2001.
January 7, 2002	**Hosting.controller.txt**	**Exploit URL for the multiple vulnerabilities in Hosting Controller v1.4.1.**
January 7, 2002	Lcrzo-4.02-src.tgz	A toolbox for network administrators and network malicious users that contains over 200 functionalities using network library lcrzo to sniff, spoof, create clients/servers, create decode and display packets, etc.
January 7, 2002	**Nt.php.htm**	**Exploit for the NT PHP.exe vulnerability.**
January 7, 2002	Ntop-2.0-src.tgz	Unix / Windows network sniffing tool that shows the network usage, which has an interactive mode and a web mode for greater functionality and options.
January 7, 2002	Webi.c	Script which exploits the HTTP Request Packet Injection vulnerability.
January 4, 2002	**Browseftp_exploit.pl**	**Script which exploits the BrowseFTP Client Buffer Overflow vulnerability.**
January 3, 2002	**Snmpx.c**	**Script which exploits the Net-SNMP snmpnetstat Remote Heap Overflow vulnerability.**
January 2, 2002	W00aimexp.tgz	Exploit for the AOL Instant Messenger Remote Buffer Overflow vulnerability.

Date of Script (Reverse Chronological Order)	Script name	Script Description
January 1, 2002	Ngrep-1.40.1.tar.gz	A powerful network sniffing tool which strives to provide most of GNU grep's common features, applying them to all network traffic.
January 1, 2002	Ritter packetsniffer20.zip	The TWLC packet sniffer for Windows 2000 / NT / XP is an advanced packet sniffer that features filtering rules, DNS lookups, interface selection, and more.
January 1, 2002	Xploit.c	Script which exploits the WinME/XP UPNP Remote DOS and Buffer Overflow Vulnerabilities.
January 1, 2002	**Zml.cgi.txt**	**Exploit URL for the Zml.cgi Multiple Remote Vulnerabilities.**
December 28, 2001	**Phrack58.tar.gz**	**Phrack Magazine Issue 58 contains: Advanced return-into-lib(c) exploits (PaX case study), Runtime binary encryption, Advances in kernel hacking, Linux on-the-fly kernel patching without LKM, Linux x86 kernel function hooking emulation, RPC without borders, Developing StrongARM/Linux shellcode, HP-UX (PA-RISC 1.1) Overflows, The Security of Vita Vuova's Inferno OS, Phrack Loopback, Phrack World News, and more.**
December 27, 2001	Smash_bin_login.c	Script which exploits the Solaris x86 v2.8 /bin/login via Telnet Remote Buffer Overflow vulnerability.
December 25, 2001	**01-wu261.tgz**	**Script which exploits the Wu-Ftpd SITE EXEC Format String vulnerability.**
December 25, 2001	Ethereal-0.9.0.tar.gz	A GTK+-based network protocol analyzer, or sniffer, that lets you capture and interactively browse the contents of network frames.
December 25, 2001	Nb-isakmp.c	Proof of concept exploit for the ISAKMP/IKE Remote Denial of Service vulnerability.
December 16, 2001	Atphttpd.pl	Perl script which exploits the ATPhttpd Remote Denial of Service Buffer Overflow vulnerability.
December 16, 2001	Atphttpd-smack.c	Script which exploits the ATPhttpd Remote Buffer Overflow vulnerability.
December 16, 2001	Skl0g.zip	Keylogger for Win32 that can log all keystrokes, is case-sensitive and supports all standard keys.

Trends

Other:

! **NIPC has updated their advisory, NIPC Advisory 01-030, regarding what Microsoft refers to as a critical vulnerability in the universal plug and play (UPnP) service in Windows. For more information see, NIPC ADVISORY 01-030.3, located at: www.nipc.gov/warnings/advisories/2001/01-030-2.htm.**

Viruses

The following virus descriptions encompass new viruses and variations of previously encountered viruses that have been discovered in the last two weeks. The viruses are listed alphabetically by their common name. While these viruses might not all be in wide circulation, it is highly recommended that users update anti-virus programs as often as updates become available. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

Carrytone (Alias: I-Worm.Taripox.b) (Internet Worm): Carrytone is a mass-mailer worm that uses a new technique to spread. The worm body is 40 kilobytes in size and it was written in C. It works properly on Windows NT based systems only. For spreading it implements a simple SMTP proxy that listens on port 25 (standard SMTP port) on the infected machine. When the worm is started, it fetches the SMTP server name from the user's e-mail settings then modifies the HOSTS file so that the SMTP server's address points to the localhost where the worm is listening. This way when the user sends an e-mail his/her e-mail client will connect to the worm instead of the real mail server. After receiving the connection, the worm relays all the commands and replies between the client and the real mail server until it gets the reply to SMTP DATA command that marks the beginning of the e-mail data. At this point it inserts a copy of itself into the message. The attachment name it uses is composed from the recipient's name and a '.doc.pif' extension. When the infected attachment is opened, it copies itself to the Windows folder as 'MMOPLIB.EXE' and adds it to the runkeys in the registry:

[HKLM]\Software\Microsoft\Windows\CurrentVersion\Run\mmopl

The worm stores some internal data under:

[HKLM]\Software\Microsoft\Media Optimization Library

JS/Gigger-A (JavaScript Virus): This is a JavaScript virus, which arrives as an e-mail message with one of the following sets of characteristics:

Subject: Outlook Express Update
Message: MSNSofware Co.
Attachment: Mmsn_offline.htm

or

Subject: recipient@Address, i.e. the e-mail address of the recipient
Message: Microsoft Outlook 98
Attachment: Mmsn_offline.htm

If the virus is executed, it will attempt to drop the following files:

! C:\Bla.hta
! C:\B.htm
! C:\Windows\Samples\Wsh\Charts.js
! C:\Windows\Samples\Wsh\Charts.vbs
! C:\Windows\Help\Mmsn_offline.htm

It will also create files called Script.ini in folders containing a file with the extension INI or HLP. These files will be detected as mIRC/Simp-Fam. The virus will infect HTM, HTML and ASP files and attempts to add the line, “Echo y|format c:” to C:\Autoexec.bat. This will have the effect of attempting to format drive C: on restart in versions of Windows that use the character Y for Yes. JS/Gigger-A creates the following registry keys:

HKCU\Software\Microsoft\Windows Scripting Host\Settings\Timeout
HKCU\Software\TheGrave\badUsers\v2.0

and adds the value 'NAV DefAlert' to the registry key:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run

Spaces (Alias: Busm) (Windows Virus): Spaces is a dangerous memory resident parasitic Windows virus. It replicates under Win95/98 only and infects Win32 executable files (PE EXE - Portable Executable). When an infected file is run, the virus installs itself into Windows memory, hooks disk file opening and infects them. The virus writes itself to the end of the file into the last file section by increasing its size. On the June 1st, the virus corrupts the MBR of the hard drive and halts the computer. The virus erases the MBR loader's code and patches the Disk Partition Table so that there is just one partition listed, and it points to the MBR sector, i.e. points to itself – the partition table loops to itself. This way of corruption is very dangerous: most of present DOSes (including MS-DOS) halts while loading - they go to unlimited loop while looking for the last disk partition. As a result, the data on the disk are not destroyed, but the disk is not accessible while loading from the floppy drive. While corrupting the MBR sector, the virus overwrites it by direct writing to the hard drive controller's ports and bypasses BIOS anti-virus protection. This routine has a bug and in some cases (depending on the system configuration) the virus causes the "General Protection Fault" error message, and this saves the MBR. The virus was named "Spaces" because is uses two spaces to detect its copy in the Windows memory (these spaces are returned by a "are-you-here?" virus function). By two spaces the virus also separates infected and not infected files - the virus writes them to the PE header to the reserved field.

SWF/LFM-926 (Shockwave Infector Virus): This is the first virus that is capable of infecting Shockwave Flash (.SWF) files, commonly used for animation and special effects on websites. When an SWF file is played, the virus displays the message "Loading.Flash.Movie..." and then it infects other SWF files in the current directory. The virus makes use of the ability of Shockwave files to run scripts. In this case it causes the command line interpreter to run a debug script which produces a file called V.COM. This file is then automatically run by the virus infecting all other SWF files in the current directory. *Note: Because the virus can spread itself using the .SWF file extension, it is recommended users add SWF to the list of file extensions to Virus scanners.*

VBS/Dismissed-A (Visual Basic Script Virus): This is a virus that was initially found on a page pointed to by the W32/Zacker-C worm. The virus spreads using network shares and attempts to spread
using mIRC. If the page is loaded using vulnerable Internet Explorer, the JavaScript code on the page drops and runs the file rol.vbs. The dropped VBS file then sets the Internet Explorer home page to point to "www.orst.edu/groups/msa/everwonder.swf." It then attempts to delete number of anti-virus product related files and directories. The virus copies itself to all files with extensions "LNK," "ZIP," "JPG," "JPEG," "MPG," "MPEG," "DOC," "XLS," "MDB," "TXT," "PPT," "PPS," "RAM," "RM," "MP3," "MDB," and "SWF" and adds extension "VBS" to the filename. It also searches for files with "HTM," "HTML," and "ASP" extensions and adds a line with code which will attempt to connect to a web page that contains the VBS/Dismissed-B virus. Finally, the virus displays a message box and attempts to shutdown Windows.

VBS/Dismissed-B (Visual Basic Script Virus): This virus is similar to VBS/Dismissed-A. Together with the complete functionality of VBS/Dismissed-A, VBS/Dismissed-B contains a routine for sending e-mail messages. The virus is initially run from an infected webpage by opening the page with a vulnerable version of Internet Explorer. To run the mailing routine, VBS/Dismissed-B drops and runs a VB
script outlook.vbs. The script then attempts to send e-mail messages using Microsoft Outlook. The subject of the message is "Very important !!!." The message body contains the text with a link that points to a
page which contains the VBS/Dismissed-B virus.

VBS/Grate-B (Visual Basic Script Worm): This worm arrives in an e-mail with the subject line "Merry
Christmas!!!" and no body text. The attachment is called greetings.txt.vbs. When executed, the worm attempts to copy itself to the Cursors folder in the Windows directory as greetings.txt.vbs. It also tries to mail itself to everyone in all Outlook address books, using the e-mail format described above, and attempts to mail PWL files to an e-mail account in Poland.

VBS/Haptime-Fam (Visual Basic Script Worm): This worm has been reported in the wild and spreads via Outlook Express version 5.0. It attempts to infect files with the extensions VBS, HTML, HTM, HTT and ASP. Most members of the VBS/Haptime family will also attempt to delete EXE and DLL files when the month plus the day are equal to 13 (for instance, June the 7th).

VBS/RTF-Senecs and Troj/Sub7-21-I (Aliases: Troj/Senecs, W32/Lastscene@mm, TROJ_SCENES) (Visual Basic Script Worm and Backdoor Trojan Horse): VBS/RTF-Senecs is a Visual Basic script worm that arrives in an e-mail message with the following characteristics:

Subject: "Scene from last weekend"
Message body: "Please do not forward"
Attached filename: scenes.zip.

The attached ZIP file contains an RTF document scenes.wri. If the document is opened, two icons are displayed for two embedded objects. Both icons appear to be icons of an image file but the actual embedded object is an executable, Troj/Senecs. If the embedded executable is launched, it drops and runs a VBS file which attempts to send scenes.zip to all contacts in the Microsoft Outlook address book. Troj/Senecs also drops two additional Trojans, Troj/Optix-03-C and Troj/WebDL-E. *Note: See Trojan Section for information on Troj/Optix-03-C, Troj/WebDL-E, Troj/Sub7-21-I.*

W32/Bomex (Aliases: I-Worm.Bormex, W32.Borm, Win32/Borm.A worm, Win32/Bormex.A@mm) (W32 Worm): This worm is typically named borm.exe. It spreads only by infecting machines that are already infected by the Back Orifice Trojan. When run, it will randomly scan the Internet for machines that are infected by Back Orifice. When it finds one, it will upload a copy of itself, and execute it on the remote machine.

W32/Donut-A (Win32 Executable file Virus): This is a .NET aware Windows file infector. When an
infected file is executed, it searches the current directory and its parent directory for executables containing .NET code. These files are modified so that Windows will treat them as standard executables and they are then infected with the virus. After infection, the virus creates a copy of itself. The filename used is created by adding a space to the end of the filename just before the extension. This file is then executed and on Windows XP may display a Message Box with the text:

This cell has been infected by dotNET virus!
.NET.dotNET by Benny/29A

On Windows 2000, the virus will recursively make a copy of itself by adding a further space into the filename and will then call this file which will create another file and so on until several hundred files are executed. This process will eventually terminate. Finally the virus creates a copy of itself which has the
original .NET code restored so that it executes as a normal .NET file. This file will have the same filename as the original infecting file, with a space added.

W32/Hybris-C (Win32 Worm): This virus has been reported in the wild. It consists of a base part and a collection of upgradeable components. The components are stored within the worm body encrypted with 128-bit strong cryptography. When run, the worm infects WSOCK32.DLL. Whenever an e-mail is
sent, the worm attempts to send a copy of itself as an attachment to a separate message to the same recipient. Any other behavior exhibited by the worm is entirely dependent on the set of installed components. The text of the e-mail message is determined by one of the installed components, and can be changed by the an upgrading mechanism. Consequently the message can have any subject, any message text, and any filename for the attached file. A common component of the worm checks the language settings of the computer it has infected, and selects a message accordingly from: English, French,
Portuguese, and Spanish. The methods for upgrading the worm can also be changed as they are also upgradeable components. At the time of writing, two have been seen. One of the upgrading techniques attempts to download the encrypted components from a website that is presumably operated by the worm author. This website has since been disabled. However, this component could be upgraded to have

a different web address. The other method involves posting its current plug-ins to the Usenet newsgroup alt.comp.virus, and upgrading them from other posts by other infections of the worm. These are again in the
encrypted form, and have a header with a four character identifier and a four character version number, in order for the worm to know which plug-ins to install. Another component of the worm searches the PC for .ZIP and .RAR archive files. When it find one, it searches inside it for a .EXE file, which it renames to .EX$, and then adds a copy of itself to the archive using the original filename. There is a payload component, which on the 24th of September of any year, or at 1 minute to the hour at any day in the year
2001, displays a large animated spiral in the middle of the screen which is difficult to close. There is also a component that applies a simple polymorphic encryption to the worm before it gets sent by e-mail. By
upgrading this component the author is able to completely change the appearance of the worm in unpredictable ways in an attempt to defeat anti-virus products detecting it.

W32/Lohack-A (Win32 Worm): This is a mass-mailing Internet worm that sends itself to e-mail addresses found by searching files on the local hard drive. It arrives as an e-mail with the following characteristics:

Subject line: Hacking course...
Message Text: Look the hacking course - version 1.0! By senna
Spy - Made In Brazil **http://www.avpavp.hpg.com.br**
Attached file: hacking.exe

The worm does not run automatically on viewing the e-mail but requires the user to double click on the attachment. W32/Lohack-A will locate the drive associated with the Windows directory and then search for files on the drive whose filesize is greater than 16 and whose file extension matches one of TXT, HTM, EML, MSG, DBX, MDX, NCH or IDX. It searches each of these files for e-mail addresses enclosed by
'<>' brackets, for example: <test@test.com> and then attempts to send itself to these addresses using MAPI based e-mail clients, such as Microsoft Outlook and Outlook Express. The worm makes no changes to the system registry and will not create or change any files.

W32/Maldal-D (Aliases: W32/Maldal.D@mm, Win32.Maldal.E) (Win32 Worm): This is a worm which spreads as an e-mail attachment. The subject of the e-mail is the name of the infected computer.
The name of the attachment is also the name of the infected computer with a .EXE extension appended to it. The e-mail message text is chosen randomly from a list. When the worm is run, it will display a fake error message. The worm will then create a copy of itself named "win.exe" in the Windows system folder and add the registry value:

HKLM\Software\Microsoft\Windows\CurrentVersion\run\System

which contains the name of the copy. The worm will also attempt to delete files used by anti-virus and other security software. It will also delete files that have the following extensions: HTM, PHP, HTML, COM, BAT, MDB, XLS, DOC, LNK, PPT, JPG, MPEG, INI, DAT, ZIP, and TXT. Finally the worm will change the name of the infected computer to: "ZaCker."

W32/Maldal-G (Alias: I-Worm.Maldal) (Win32 Worm): This worm has been reported in the wild and spreads as an e-mail attachment. The subject of the e-mail is "ZaCker." The name of the attachment is "ZaCker.exe." The e-mail message text is chosen randomly from a list. When the worm is run, it will display a fake error message. The worm will then create a copy of itself named "win.exe" in the Windows system folder and add the registry value:

HKLM\Software\Microsoft\Windows\CurrentVersion\run\System

which contains the name of the copy. The worm will also attempt to delete files used by anti-virus and other security software. It will also delete files that have the following extensions: HTM, PHP, HTML, COM, BAT, MDB, XLS, DOC, LNK, PPT, JPG, MPEG, INI, DAT, ZIP, and TXT. Finally the worm will change the name of the infected computer to "ZaCker."

W32/Shatrix-A (Win32 Worm): This is an e-mail worm that spreads as an e-mail attachment. The e-mail subject is: "FW:Shake a little." The worm is in an attachment named Shake.exe. When the worm is run, it will cause a window to move randomly around the screen for a few seconds. It then copies itself, using a random name, to the Windows system directory and adds a registry value to:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\SystemInfo

or

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\SystemInfoM

which contains the name of the copy. The worm will also look for files with .HTM, .HTML and .ASP extensions in the directory \inetpub\wwwroot. If it finds such files, it will edit them so that they include one or more messages.

W32/Shoho-A (Aliases: W32/Shoho@mm, I-Worm.Welyah) (Win32 Worm): This is a worm which spreads by exploiting a security vulnerability detailed in Microsoft Security Bulletin MS01-027 at **http://www.microsoft.com/technet/security/bulletin/MS01-027.asp**. The worm spreads as an attachment to an e-mail with the subject:

"Welcome to Yahoo! Mail"

The attachment is named "readme.txt<large number of spaces>.pif." This may cause the attachment to be run when the e-mail is viewed. When the worm is run, it will create copies of itself named Winl0g0n.exe in the Windows and Windows system directories. It will also create the file e-mail.txt containing a copy of the e-mail message used by the worm. The worm then creates the registry values:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Winl0g0n.exe

and

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Winl0g0n.exe

both of which contain the path and filename of a copy of the worm. This ensures that the worm is run the next time Windows is started. The worm then searches the hard disk for addresses to which it can send itself. It will also delete files at random from the directory in which it is running. Note that when the computer is restarted, the worm will be run in the Windows directory and may delete files that are required for the correct operation of Windows.

W32/Shoho-Fam (Aliases: W32/Shoho@mm, I-Worm.Welyah) (Win32 Worm): This worm has been reported in the wild. The majority of viruses in the W32/Shoho family conform to the following description. W32/Shoho is a worm that spreads by exploiting a security vulnerability detailed in Microsoft Security Bulletin MS01-027 at **http://www.microsoft.com/technet/security/bulletin/MS01-027.asp** that may cause the worm to be run when an infected e-mail is viewed. (The patch described in the security bulletin fixes a number of vulnerabilities in Microsoft's software, including the one exploited by this worm.) The worm spreads as an attachment to an e-mail with the subject: "Welcome to Yahoo! Mail." The attachment is named: "readme.txt<large number of spaces>.pif." When the worm is run, it will create copies of itself named "Winl0g0n.exe" in the Windows and Windows system directories. It will also create the file, e-mail.txt, containing a copy of the e-mail message used by the worm. The worm then creates the registry values:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Winl0g0n.exe

and

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Winl0g0n.exe

both of which contain the path and filename of a copy of the worm. This ensures that the worm is run the next time Windows is started. The worm then searches the hard disk for addresses to which it can send itself. It will also delete files at random from the directory in which it is running. Note that when the computer is restarted, the worm will be run in the Windows directory and may delete files that are required for the correct operation of Windows.

W32/Spester@MM (W32 Worm): This mass-mailing worm also spreads via Internet Relay Chat. It poses as a mouse speed test game. The worm arrives in an e-mail message with the attachment, spdtest.zip. (The .ZIP file carries an .EXE that creates an .INI file and a .VBS file. The VBS file is responsible for mailing the .ZIP package out to others.) When the .ZIP attachment is opened and the contents are extracted and run, a "game" is played. The challenge is for you to click a button with your mouse. However, the button moves away from your pointer as soon as it is placed over the button. Various taunting messages are displayed within the button as the game progresses. Finally, one big button, which does not move is displayed. Once clicked, a message box is displayed. Clicking that button results in a bogus Formatting C drive progress bar. After a few seconds, a message box appears stating that the drive was not formatted. The virus creates a VBScript file to carry out its mailing routine, "C:\Program Files\Internet Explorer\oneclock.vbs." This VBS file sends the virus to all users found in the Microsoft Outlook Address book using MAPI. The script has some date activated payloads. On the 10th day of the month, a message box is displayed which reads "Tip Of The Day: You look really beautiful today." On the 25th day of the month, the message is only sent to 1 recipient. On the 31st day of the month, 51 directories are created, 91 directories are created, 131 directories are created, and the message is sent to only 1 recipient. On September 12th, a message box is displayed which reads "Happy Birthday!!!" The files create a marker file which it uses to know if it has e-mailed its message out: C:\Program Files\Common Files\one.dat. The C:\mIRC\SCRIPT.INI file is overwritten with instructions to send C:\MIRC\SPDTEST.ZIP to IRC users when joining the channel that an infected user is on.

W32/Toget@MM (Win32 Worm): This mass-mailing worm is written in Microsoft Visual Basic and is UPX packed. It sends itself to all users in the Microsoft Outlook Address book, alters the desktop wallpaper, and tries to disable certain anti-virus software. It arrives in an e-mail message with the attachment, NUDEPIC.JPG.EXE. Running the attachment infects the local machine. The worm attempts to send itself to all users found in the Microsoft Outlook Address book and to kill the following processes:

- AVP Monitor
- F-STOPW Version 5.06c
- NAI_VS_STAT
- vettray

The file C:\WINDOWS\wallpaper.html is created which contains the text: "I want a girl with big buttocks, like Irina..." This text is displayed on the desktop if Active Desktop is enabled.

W32/Zacker-C (Aliases: W32/Maldal.c@MM, W32/Reeezak.A@mm, I-Worm.Keyluc) (Win32 Worm): This worm has been reported in the wild. It attempts to spread using Microsoft Outlook or Microsoft Messenger. When first run, the worm copies itself into the Windows directory as Christmas.exe and creates the registry entry:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Zacker = <Windows>\Christmas.exe,

so that it is run automatically each time Windows is restarted. The worm changes the computer name by setting the registry key:

HKLM\System\CurrentControlSet\Control\ComputerName\ComputerName\ComputerName = Zacker

and changes the default browser home page by setting the registry key:

HKU\.DEFAULT\Software\Microsoft\Internet Explorer\Main\Start Page

to point to the geocities website. W32/Zacker-C also attempts to disable the keyboard.

WM97/Ded-V (Word 97 Macro Virus): This virus has been reported in the wild. It is a Word macro virus, which infects Microsoft Word documents. The virus has been created by an interaction between two other Word macro viruses: WM97/Ded-B and WM97/Class.

WM97/Marker-JY (Word 97 Macro Virus): WM97/Marker-JY creates the non-viral file C:\himem.sys, which it uses to replicate. If an attempt is made by the user to access the macros in infected documents, then the message 'Configuration error, please reinstall Microsoft Word' is displayed.

Weird (Alias: Win32.Weird) (Win32 Virus): This is a memory resident parasitic Win32 virus. It is not dangerous and writes itself to the end of PE EXE files (Windows executable) by increasing the last file section and modifying PE header fields. The virus copy consists of two parts. The first part (starter) is a short routine, and the second part is the main virus code encrypted with a silly encryption loop. When the infected file is executed, the starter takes control, decrypts the second part of virus code, drops it to Windows directory as a PE EXE file with a random name and executes it. The main virus instance stays memory resident as a hidden Windows application, runs a low priority thread that periodically scans drives' directory trees, looks for PE EXE files, and infects them. The virus also affects the EXPLORER.EXE file. It copies it with the EXPLORER.E name, infects this copy, and writes the [rename] instruction to the WININIT.INI file to replace the original EXPLORER.EXE with the infected copy on the next Windows startup. The virus has a backdoor ability. When it is active as a Windows application, it opens the Internet connection and waits for specific calls from there. The virus has a small list of supported commands compared to other known backdoors, but it allows a malicious user to upload, download, execute, and delete files on the infected machine from remote host. The virus contains the "copyright" text: “#Coded by Weird#.”

WORM_MALDAL.D (Aliases: MALDAL.D, MALDAL, W32.Maldal.D@mm) (Internet Worm): This is a destructive, memory-resident worm that uses Microsoft Outlook to propagate via e-mail. It copies itself to a WIN.EXE file in the System directory and deletes antivirus programs and certain files.

WORM_MALDAL.E (Aliases: MALDAL.E, MALDAL) (Internet Worm): This worm is a variant of WORM_MALDAL.C and WORM_MALDAL.D. It propagates via e-mail using Microsoft Outlook. It has a destructive payload that deletes antivirus software and other files.

WORM_GOP.A (Aliases: W32.HLLW.GOP, W32/GOP-A, Trojan.PSW.Gop.196, PSW.GOP.196, GOP.A): This Win32 worm uses its internal SMTP engine to propagate copies of itself via e-mail. It arrives in an HTML formatted e-mail with a random subject and message body (usually in Chinese). It arrives as an attachment that carries a double extension (e.g. FILE.TXT.EXE, FILE.DOC.EXE, FILE.BMP.EXE, etc.). It uses a known vulnerability in Internet Explorer-based e-mail clients to execute the file attachment automatically on unpatched systems. This vulnerability is known as Automatic Execution of Embedded MIME type.

WORM_ZOHER.A (Aliases: ZOHER.A, ZOHER, W32/Sheer.A@mm, W32.Zoher@mm.html) (Internet Worm): Upon execution, this worm connects to a Web site and downloads a text message. The text message contains the e-mail message and the subject that this worm arrives with. By default, it arrives in an e-mail with the subject "fw: Scherzo." The e-mail message is in MIME format and contains an embedded copy of the worm. The worm propagates by sending e-mail to all addresses listed in the infected user's Windows Address Book, via the default SMTP server. It uses a known Internet Explorer vulnerability to automatically execute the file attachment. This worm does not affect Windows NT or XP systems. *Note: It is important that all e-mail users download the MIME Header Microsoft patch because without it a computer can be infected by merely viewing the worm e-mail message in Microsoft Outlook or Outlook Express.*

X97M/Ellar.b (Aliases: Excel97Macro/Ellar.B, Macro.Excel97.Ellar.b, X97M.Ellar.B) (Excel 97 Macro Virus): This virus propagates by infecting Excel workbooks in Microsoft Excel 97 and higher. This virus will suppress alert messages and disable the Macro Warning protection. It copies itself to the XLStart folder as %Computer Name%.xls or MICROSOFT.XLS. If the day of the week is divisible by 3, then XLS and MDB files are deleted from the current directory and sub directories on fixed and network drives. It may hide or change the order of worksheets as well.

XM97/Bdoc2-A (Excel 97 Macro Virus): This virus creates the file, AutoRun.xla, in the XLSTART directory. On the 26th April it may display a message in non-Roman characters. If the day of the month is a multiple of 5, then the virus will terminate the current Windows session.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table starts with Trojans discussed in CyberNotes #2001-01, and items will be added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. *Note: At times, Trojans may contain names or content that may be considered offensive.*

Trojan	Version	CyberNotes Issue #
Backdoor.Palukka	**N/A**	**Current Issue**
DlDer	**N/A**	**Current Issue**
JS/Seeker-E	**N/A**	**Current Issue**
JS_EXCEPTION.GEN	**N/A**	**Current Issue**
SecHole.Trojan	**N/A**	**Current Issue**
Troj/Download-A	**N/A**	**Current Issue**
Troj/Optix-03-C	**N/A**	**Current Issue**
Troj/Sub7-21-I	**N/A**	**Current Issue**
Troj/WebDL-E	**N/A**	**Current Issue**
TROJ_DANSCHL.A	**N/A**	**Current Issue**

Backdoor.Palukka: This is a backdoor Trojan horse that can give a malicious user access to the computer. Like many other backdoor Trojans, Backdoor.Palukka is controlled using IRC channels. This particular backdoor Trojan provides a great deal of control over a compromised computer, including file system access and the ability to use the compromised computer in a distributed Denial of Service attack.

DlDer (Aliases: Trojan.Win32.DlDer, Troj_DlDer): This is a two-component spyware-trojan. It was supposed to be an on-line lottery game with an adware component that had to display advertisement and offers. But the way it was implemented and dropped to users' systems made anti-virus vendors consider it a spyware-trojan. Do note that DlDer is NOT a virus, as it doesn't spread. The Trojan being installed on a user's system downloads or upgrades its main component that connects to a website and reports user's ID (unique for each computer), IP address, web browser a user is using and URLs that a web browser opens. The DlDer spyware-trojan was installed with LimeWire, Kazaa, Grokster and some other software packages that are mainly used for user-to-user file exchange purposes (now most of these packages are distributed without DlDer Trojan components). The Trojan was installed even if a user selected not to install any additional (spyware) components from those packages during setup phase or was just hiddenly dropped to a user's system. The main component of the Trojan is Explorer.exe file that is located in main Windows folder in \Explorer\ subfolder (do not mix with the original Windows' Explorer.exe that is located in main Windows folder, usually C:\Windows or C:\WinNT). This component is downloaded or upgraded by the second Trojan component (downloader) that has the name 'DlDer.exe' and is located in main Windows folder. The DlDer.exe Trojan component when it is started after installation of the above listed software packages, downloads Explorer.exe file from a website and puts it to \Explorer\ subfolder of main Windows folder. Then the Trojan creates a startup key for the downloaded Explorer.exe file. On next system restart the Explorer.exe file is activated and it creates a startup key for DlDer.exe file (Trojan components activate each other). Then Explorer.exe starts to regularly connect to a website and report user's ID (unique number), IP address, web browser and URLs that a user visits to that site.

JS/Seeker-E: This Trojan has been reported in the wild. It is a malicious script which exploits a security
vulnerability detailed in Microsoft Security Bulletin MS00-075. It will attempt to modify Internet Explorer settings, such as the Start Page and Search setting, to overwrite installed values. Generally the new settings point to sites which are pornographic in nature. The Trojan writes to Registry values under, HKCU\Software\Microsoft\Internet Explorer.

JS_EXCEPTION.GEN (Aliases: Trojan.Seeker-based, HTML.VMExploit, JS.Exception.Exploit, EXCEPTION, EXCEPTION.GEN, Coolsite, Coolsite.A, JS/Coolsite.A): This Java Script Trojan changes the infected user's Internet Explorer startup page. Other samples (Coolsite samples) are mass-mailers. It exploits security vulnerabilities in the Microsoft Virtual Machine. Some variants have non-destructive payloads that change the button caption, modify the appearance of Internet Explorer, and redirect links to a certain Web site.

SecHole.Trojan: This is a Trojan that can be used to by a malicious user that does not have administrator rights to gain full control on computers running Windows NT 3.51 and 4.0. It is similar to a hacktool. When it is executed, the malicious user can run some code in the system security context and thereby obtain local administrative privileges on the system. This security hole occurs only on computers that are running Windows NT 3.51 and 4.0. To fix this security hole, make sure that you have obtained all service packs and patches for these operating systems. For more information please see Microsoft Security Bulletin (MS98-009) located at:
http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/bulletin/ms98-009.asp.

Troj/Optix-03-C: This is a backdoor Trojan horse loaded by the VBS/RTF-Senecs worm that will run in the background as a server process, allowing a remote malicious user (using a client program) to gain access and control over the machine. When first run, it creates the subdirectory <Windows>\OleFiles\, moves itself there and creates the Registry entry:

> HKLM\Software\Microsoft\Windows\CurrentVersion\explorer\User Shell Folders\Common Startup = <Windows>\OleFiles\<Trojan name>.

This ensures that the server process is run automatically each time the machine is restarted.

Troj/Sub7-21-I: This is a backdoor Trojan horse. When the server program is installed, the computer is exposed to security attacks from remote locations. Once the connection is established, the attacker can acquire sensitive information such as passwords and take control over the infected computer.

Troj/WebDL-E: This is a Trojan loaded by the VBS/RTF-Senecs worm that attempts to download and run a program from a website hosted at tripod.com. The downloaded program is the Troj/Sub7-21-I Backdoor Trojan horse. Troj/WebDL-E will also attempt to send a notification message of its success to an ICQ account. After running, the Trojan horse removes itself from the system.

TROJ_DANSCHL.A (Aliases: DANSCHL.A, Trojan.Win32.Malantern, Danschl, W32/Danschl.A, Trojan/Win32.Danschl.A, Win32.Danschl.A, Trojan.Danschl.A): This Trojan deletes SYS files from the %Windows%\System32\Drivers directory and creates new folders in the Desktop and %Windows% directory. It is the directory where Windows folder is located. This is usually in the C:\Windows. Upon execution, this Trojan also displays several message boxes containing text that claims to be from the FBI.